ITEA Journal 2010; 31: 473–477

The Information Assurance Range

Robert Powell
Defense Information Systems Agency, Falls Church, Virginia
Timothy K. Holmes
Joint Interoperability Test Command, Indian Head, Maryland
Cesar E. Pie
Cyber security Research and Solutions Corporation, La Plata, Maryland

An effective Information Assurance (IA) posture is achieved when there is confidence that information and information systems are protected against attacks through the application of security services in such areas as availability, integrity, authentication, confidentiality, and non-repudiation. All Department of Defense (DoD) organizations must expect attacks and must incorporate attack-detection tools and procedures that allow them to react to and recover from these incidents and events while still achieving mission success. Since technical mitigations are of no value without trained people to use them and operational procedures to guide their application, it is paramount that in implementing an effective and enduring IA framework, DoD organizations achieve a balance from all three facets of a Defense in Depth strategy: people, operations, and technology. The IA Range seeks to satisfy this strategy.

Key words: CND tactics; computer network defense; IA range; information assurance; T&E.

Cyber threats are asymmetric, surreptitious, and constantly evolving—a single individual or non-state sponsored group anywhere in the world can inexpensively and secretly attempt to penetrate systems containing vital information or mount damaging attacks on critical infrastructures. Moreover, the pervasive interconnectivity of the Global Information Grid (GIG) makes cyber attacks an increasingly attractive prospect for first, second, and third generation threats and adversaries.

In light of the current operational threat environment, the deliberate investments of time, resources, and attention in implementing and maintaining an effective Information Assurance (IA) posture have never been more important or more challenging. The IA Range provides an operational representation of today's GIG IA architecture within a Network Operations (NetOps) construct. Unlike theoretical models, the IA Range is an infrastructural platform designed to integrate distributed and heterogeneous IA architectural systems and solutions with the Department of Defense (DoD) Computer Network Defense (CND) operational hierarchy. The IA range provides DoD stakeholders with an avenue to strengthen the GIG security posture by supporting operational exercises, training network defenders, and testing and evaluating new information capabilities.

Test and Evaluation (T&E) mission

In support of its T&E mission, the IA Range incorporates Defense in Depth design principles to provide DoD organizations with a methodical, repeatable, and verifiable Cyber T&E framework (supported by performance-based metrics indicators) to measure (i.e., quantify and qualify) the abilities and capabilities of network defenders to synergistically integrate *people*, *operations*, and *technology* to *protect*, *monitor*, *detect*, *analyze*, *diagnose*, and *respond* (i.e., contain, eradicate, and recover) to cyber security attacks. In addition to providing for a realistic T&E environment that is segregated from the operational environment (reducing the IA risk and minimizing the technical and operational impacts to zero), the IA Range, as a capability, provides DoD organizations with a venue to measure the cyber security workforce operational performance, the adequacy of in-place cyber security services (near term CND tools and mechanisms), and validate established and mandated IA and CND tactics, techniques, and procedures.

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2010		**00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Information Assurance Range	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Defense Information Systems Agency,Falls Church,VA,22041**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**5**	

T&E objectives

The IA Range framework will be used to promote a consistent, repeatable, and verifiable T&E venue by which IA and Computer Network Operations (CNO) technical and operational concepts can be validated against requirements and specifications for improvement. Specifically, the IA Range will seek to achieve the following T&E objectives:

- improve cyber security workforce operational performance,
- validate capabilities and services provided by CND tools and mechanisms,
- validate and improve CND tactics, techniques, and procedures,
- validate acceptable level of service of Computer Network Defense Service Providers (CNDSPs), and
- validate IA mitigation strategies for programs of record.

The cyber threat

The cyber threat environment is very dynamic and complex. This environment is predominantly used by well-funded adversaries with strong economic and political motivations and powerful technical capabilities. Today, foreign nations represent the most sophisticated threat. Foreign nations have learned to recognize the value of attacking adversary computer systems, both on the military and domestic front. Foreign nations are currently improving their doctrine and dedicated government-sponsored offensive cyber warfare programs. They are supported by institutional processes and significant resources and have begun to include information warfare in their military doctrine. The second most sophisticated threat and next group of potential adversaries comprises primarily non-state actors who present the most diverse and difficult threat entity to characterize. Non-state actors, including terrorists, have come to recognize that cyber weapons offer them new, low-cost, easily hidden tools to support their causes. The skills and resources of this threat group range from the merely troublesome to dangerous, and while they are unlikely to mount an attack on the same scale as a nation, they can still do considerable harm. The least sophisticated threats are lone or possibly small groups of amateur hackers without significant resources. These inexperienced malicious hackers use common hacker tools and techniques in an unsophisticated manner to attack computer systems and are the source of most attacks.

Improve cyber security workforce operational performance

As shown in *Figure 1*, the IA Range promotes improved cyber security workforce operational performance through performance metrics to measure both a simulated opposing force's cyber attack activities and friendly network defenders protecting, monitoring, detecting, analyzing, diagnosing, and responding to the cyber attacks. Strategically, an Opposing Force (OPFOR) is employed in this environment to execute cyber attack scenarios. The steps a hacker may follow will be broadly divided into seven phases, which include footprinting and scanning, enumeration, gaining access, escalation of privilege, maintaining access, network exploitation, and covering tracks. This is the most effective framework to test network defenders because it forces the warfighter to consider all aspects of an attack—the best way to defend our networks is to think like the enemy. Defined by DoD requirements, these scenarios will be strategically designed to exercise different classes of attacks (e.g., passive, active, insider, close in, distribution) and their corresponding threats (i.e., nation state, non-nation state, etc.). Every scenario includes elements such as the expected actions, conditions, standards, operational threat environment options, associated risks, event stoppers, and applicable training audience. If successful, the OPFOR will challenge security assumptions and strategies, expose operational and technical weaknesses, and stimulate fresh thinking about the enterprise security posture. This construct provides a simplistic approach, agile and flexible enough to be expanded into a more complex assessment model.

Validate capabilities and services provided by CND tools and mechanisms

A CND tool or mechanism is a device that provides one or more of the following capabilities and services: protection, monitoring, detection, analysis and diagnosis, and/or responding (i.e., containing, eradicating, and recovering) from incidents and events. To support CND emerging technologies, the IA Range provides a stable environment to more effectively and efficiently improve the design, implementation, and calibration of new CND technologies. This includes validating the capabilities and services provided by these devices as well as the implications and tradeoffs of implementing different and alternative security technology strategies throughout the GIG.

In addition, since the scale, complexity, and diversity of the components, systems, infrastructures, and operational environments comprising the GIG are unprecedented in the DoD, no one solution fits all; yet all solutions must adhere to a common set of guiding principles, common lexicon, and consistent set of capabilities and activities that govern system design and evolution, thus enabling interoperability. With this in mind, the IA Range provides an ideal environment

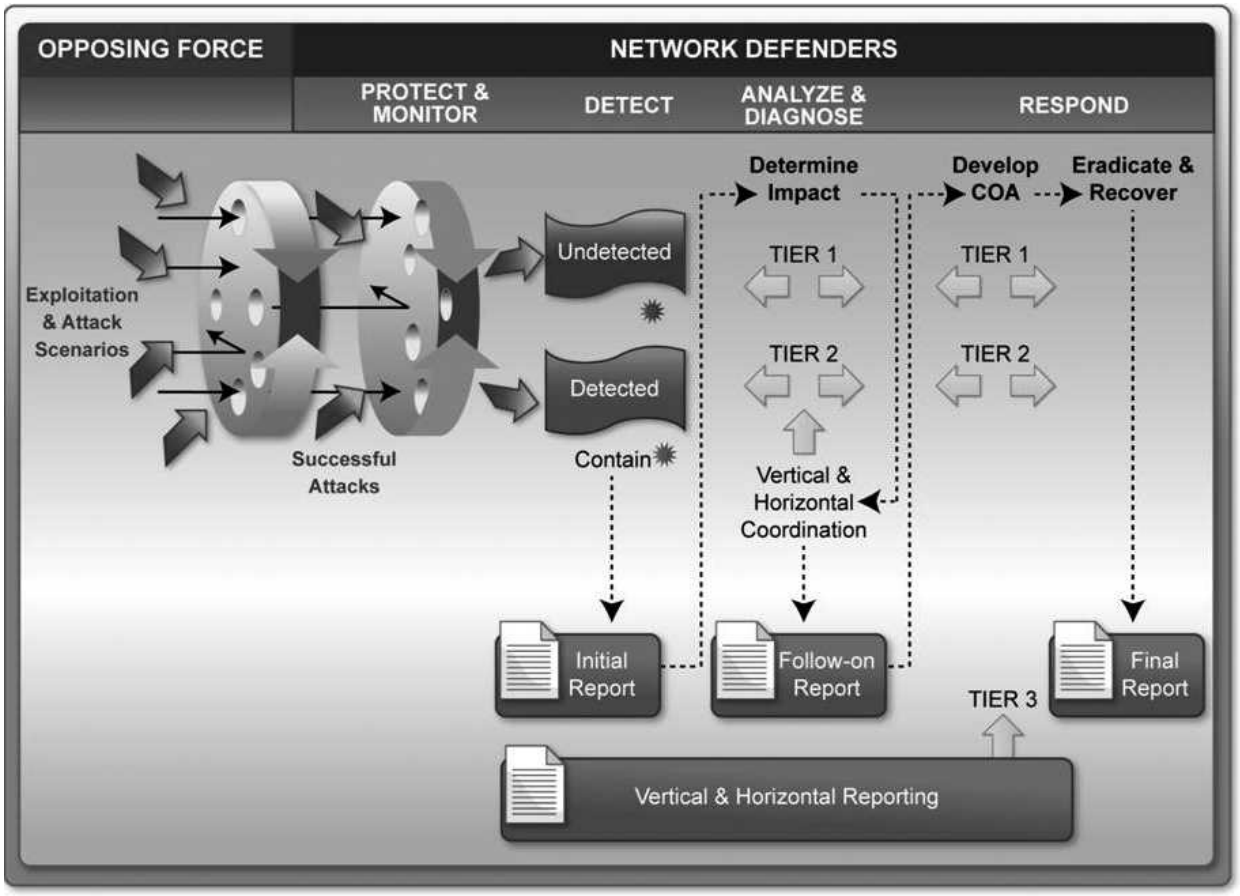

Figure 1. Cyber security assessment framework.

for testing the effectiveness and efficiency of tools and technologies, both for the purpose of improving technologies still in the research and development stages and for testing existing deployed mechanisms, thus validating architectural models of IT systems and infrastructure at large scales (i.e., Demilitarized Zone). This ensures that individually and collectively, CND tools and mechanisms contribute to the overarching DoD strategic IA plan; support the full spectrum of solutions involving any combination of doctrine, organization, training, materiel, leadership and education, personnel and facilities; and promote the maturity of these capabilities from concepts to realized Defense in Depth capabilities.

Validate and improve CND tactics, techniques, and procedures

When implementing CND technologies, it is important to note that each element of the *people*, *operations*, and *technology* triad plays a role in the cyber security of critical infrastructures. Well-documented Tactics, Techniques, and Procedures (TTPs) can often help to overcome potential vulnerabilities in a security product, while poor implementation can render good technologies ineffective. In order to mitigate risk and operate DoD networks in an organized and cohesive way, it is important to lay the framework for operation and administration of CND. The efforts from this strategic area help the warfighters effectively fight cyber threats by ensuring clear guidance, consistency of operations, and high readiness throughout the DoD enterprise.

In support of this effort, the IA Range will be used to validate and improve CND TTPs across the enterprise and achieve an optimal readiness posture. The IA Range can influence the development of TTPs necessary to systematically implement IA and CND for the GIG. Identification and establishment of standard TTPs are a critical initial step in deploying cyber security solutions to meet GIG operational requirements. In a net-centric environment, TTP development needs to be dynamic and aligned with GIG IA and CND activities and technology advances to maximize the benefits of achieving the GIG vision. As the technology evolves, supporting TTPs must be updated accordingly to complement the emerging technological capabilities.

Validate acceptable level of service of CNDSPs

DoD Manual O-8530.1-M, "*Computer Network Defense Service Provider Certification and Accreditation Process*," defines a measurement-driven Certification and Accreditation (C&A) process for evaluating the performance of DoD CNDSPs. The term CNDSP is used to describe the providers of CND and incident response services in DoD that incorporate services similar to those provided by Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs). Unlike traditional C&A, which calculates the security risk for a given system and certifies that the security controls in place for that system adequately mitigate that risk, the C&A of a CNDSP assesses the degree to which that provider assures a minimum standard of service to its DoD subscribers. Assuming specific GIG architectural design requirements, the IA Range could be used to validate that general CNDSP services meet predefined criteria. These criteria could be captured for example by utilizing metrics to measure the adequacy of the services the CNDSPs provide in four main categories:

- **Protect**—includes vulnerability analysis and assessment, CND red teaming, virus protection, subscriber protection and training, information operations condition implementation, and IA vulnerability management;
- **Monitor**, **Detect**, **Analyze and Diagnose**—includes network security monitoring and intrusion detection; attack sensing, warning, and indications; and situational awareness;
- **Respond**—includes containment, eradication, recovery, and incident reporting;
- **Sustain Capability**—includes memoranda of understanding and contracts; CND policies and procedures; CND technology development, evaluation, and implementation; personnel levels and training/certification; security administration; and the primary information systems that support the CNDSP.

Validate IA risk mitigation strategies for programs of record

The IA Range can be an effective tool for evaluating complex programs of record. Programs of record may encompass globally distributed systems, through numerous distributed organizations, a wide range of technologies, and the effects of interdependencies among systems. The IA Range can facilitate validation of recurring IA mitigation strategies and improve Programs of record capabilities and effectiveness. IA risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls (recommended from the risk assessment process). Because the elimination of all risk is usually impractical or close to impossible, the IA Range could be used, for example, to validate the least-cost approach and the most-appropriate controls to decrease mission risk to an acceptable level, with minimal adverse effect on GIG resources and mission.

In addition, because of a Defense in Depth strategy, in the context of the DoD IA C&A process, the IA Range could be used to validate IA control inheritance. IA control inheritance is a common state in which an IA control, along with the control's validation results and compliance status, is passed, or "inherited," from an originating Information System (IS) to a receiving IS for the purposes of C&A. The sharing of IA control compliance status and evidence allows C&A practitioners to model an environment where security mechanisms are shared across multiple ISs. Inheritance eliminates testing redundancy by passing the actual results, associated validation artifacts, and compliance status from the originating IS to each inheriting IS. The IA Range could be used to validate some of these test results.

Conclusion

The DoD IA Range will surely prove invaluable for warfighting organizations looking to measure the effectiveness of enterprise tools and TTPs prior to their release into the production network. The realistic operational environment offered by the IA Range can be custom tailored to meet the assessment needs of a small-scale test effort, as well as a larger-scale enterprise program of record evaluation that requires multiple tools, services, and agency participants. It will strengthen IA awareness and the overall security posture of networked systems throughout the DoD. ❑

Mr. Robert Powell hangs his hat at the Defense Information Systems Agency's office of Field Security Operations, Arlington, Virginia, and is the program manager for the DoD IA Range. Mr. Powell is a summa cum laude graduate of Shenandoah University, Winchester, Virginia, and holds numerous industry certifications to include the Certified Information Systems Security Professional. E-mail: robert.powell@disa.mil

Mr. Kevin Holmes serves as the Joint Interoperability Test Command (JITC) information assurance technical advisor, where he develops and maintains the Command's IA policies, methodologies and capabilities. Mr. Holmes joined the JITC shortly after its inception in 1989. He has held a variety of positions within the Command. Mr.

Holmes started his JITC career developing software for many JITC instrumentation systems; ranging from tactical message protocol analyzers to modeling and simulating tactical data systems. He stood up the JITC IA capability in 2001 and has been working in that area since. Holmes earned his bachelor of science degree in management information systems (MIS) from the University of Arizona and his master of science degree in computer science from George Mason University. E-mail: kevin.holmes@disa.mil

Mr. Cesar E. Pie is chief executive officer of Cyber Security Research and Solutions Corporation (CSRS-Corp). He has extensive program management expertise and has provided subject matter expert support to the JITC for over 6 years in the fields of information system security engineering, information assurance, and computer network operations (computer network attack, computer network exploitation, and computer network defense). Mr. Pie graduated from the University of Maryland University College with a master of science degree in Computer System Management—Information Assurance Program. This program is supported by the Department of Homeland Security and the National Security Agency's Center of Academic Excellence in Information Assurance Education (CAE/IAE). Among others, a few of Mr. Pie's certification credentials include Certified in the Governance of Enterprise Information Technology (CGEIT), Information System Security Engineering Professional (ISSEP), Certified Information Systems Auditor (CISA), Certified Information System Security Professional (CISSP), and Project Management Professional (PMP). E-mail: cesar.pie@csrscorp.com

References

DoD. 2003. *Department of Defense Computer Network Defense Service Provider Certification and Accreditation Manual,* O-8530.1-M. Washington, DC: DoD.